Транспортное право и безопасность. 2024. № 4(52). С. 135—150.
Transport law and security. 2024; (4(52)):135—150.

ПРАВОВЫЕ ОСНОВЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ
LEGAL FRAMEWORK OF NATIONAL SECURITY

Научная статья
УДК 341.231:004

Legal Challenges to Cyber Sovereignty

Mahmoud Ismail,
PhD in Law, Associate Professor,
Applied Science Private University
Amman, Jordan

Al Ali Naser Abdel Raheem,
PhD in Law, Associate Professor,
Russian University of Transport (MIIT),
Moscow, Russia

Noor Saleh Ali Alzyoud,
PhD in Law, Associate Professor,
Philadelphia University
Amman, Jordan

Vladimir Ev. Chebotarev,
Candidate of Economic Sciences, Associate Professor,
Russian University of Transport (MIIT),
Moscow, Russia

Abstract. The study discusses the legal challenges imposed by cyberspace on the concept of sovereignty in international and national law, focusing on two main issues: challenges associated with the concept of sovereignty and those related to its implementation. Cyberspace presents legal challenges to state sovereignty, as the openness of cyberspace contradicts the closed nature required by traditional sovereignty. Globalization exacerbates these challenges, as supranational governmental structures and societies seek to exploit cyberspace for economic and cultural purposes, increasing the conflict between sovereignty and cyberspace openness. Defining cyber sovereignty requires a balance between the concepts of sovereignty and cyberspace to maintain their identities and characteristics. A careful definition of cyber sovereignty contributes to understanding the actual ex-tent of state authority in controlling and regulating cyberspace and helps address the legal challenges

faced by states in this context. The study concludes that cyber sovereignty is an application of sovereignty in the traditional sense, rather than a synonymous concept, and calls for international recognition of this new application and collaborative efforts to regulate it to address emerging challenges in cyberspace and ensure global security and stability.

Keywords: legal challenges; cyber sovereignty; cyberspace; traditional sovereignty; power of attorney; international law; international sovereignty.

Правовые проблемы киберсуверенитета

Махмуд Исмаил,
кандидат юридических наук, доцент,
Частный университет прикладных наук,
Амман, Иордания

Аль Али Насер Абдель Рахим,
кандидат юридических наук, доцент,
Российский университет транспорта (МИИТ),
Москва, Россия

Нур Салех Али Альзиуд,
кандидат юридических наук, доцент,
Филадельфийский университет
Амман, Иордания

Чеботарев Владимир Евгеньевич,
кандидат экономических наук, доцент,
Российский университет транспорта (МИИТ),
Москва, Россия

Аннотация. В исследовании рассматриваются правовые проблемы, которые киберпространство налагает на концепцию суверенитета в международном и национальном праве, уделяя особое внимание двум основным вопросам: проблемам, связанным с концепцией суверенитета, и проблемам, связанным с ее реализацией. Киберпространство вызывает правовые проблемы для государственного суверенитета, поскольку открытость киберпространства противоречит закрытой природе, требуемой традиционным суверенитетом. Глобализация усугубляет эти проблемы, поскольку наднациональные правительственные структуры и общества стремятся использовать киберпространство в экономических и культурных целях, усиливая конфликт между суверенитетом и открытостью киберпространства. Определение киберсуверенитета требует баланса между концепциями суверенитета и киберпространства для сохранения их идентичности и характери-

стик. Четкое определение киберсуверенитета ведет к пониманию фактического объема полномочий государства в процессе контроля и регулирования киберпространства и помогает решать правовые проблемы, с которыми сталкиваются государства в этом контексте. В исследовании делается вывод, что киберсуверенитет представляет собой применение суверенитета в традиционном смысле, а не синонимичное понятие, и содержится призыв к международному признанию этого нового применения и совместным усилиям по его регулированию в целях решения возникающих проблем в киберпространстве и обеспечения глобальной безопасности и стабильности.

Ключевые слова: правовые проблемы; киберсуверенитет; киберпространство; традиционный суверенитет; доверенность; международное право; международный суверенитет.

Для цитирования: Mahmoud Ismail, Al Ali Naser Abdel Raheem, Noor Saleh Ali Alzyoud, Chebotarev Vladimir Ev. Legal Challenges to Cyber Sovereignty // Транспортное право и безопасность. 2024. № 4 (52). С. 135—150.

1. Introduction

The cyber environment presents legal challenges to state sovereignty, stemming from the inherent contradiction between the openness of cyberspace and the closed nature required by traditional sovereignty. These challenges have emerged within the contemporary legal philosophy amidst globalization, where supra-governmental structures seek profit and market exploitation, while societies utilize cyberspace for communication and cultural exchange [1].

However, this openness also poses threats across borders, affecting both state structures and societal norms. The problem posed by cyberspace is the absence of borders, and even though the primary driving force behind technology is commerce, not politics; we can argue that the original developers of internet technology were touched by a political agenda to accommodate the interests of capitalists. Their objective was to limit state authority by establishing a decentralized network that interconnected the entire globe without a central controlling node [2]. Yet, the cyberspace has significantly diminished the role of states in regulating cyberspace interactions.

Consequently, questions arise regarding the extent and nature of international sovereignty in an increasingly interconnected world, highlighting the need to delineate the actual extent of state authority in regulating cyberspace within national borders. To achieve this, a careful definition of cyber sovereignty is necessary, balancing the concepts of sovereignty and cyberspace to avoid compromising the identity and characteristics of either.

Kuehl (2009) defines cyberspace as a global domain within the informational environment, distinguished by its unique nature, shaped with electronics and the electromagnetic spectrum for creating, storing, modifying, exchanging, and exploiting information across interconnected networks using communication and information technologies. Sovereignty, meanwhile, remains a stable concept in the current internation-

al system, closely associated with the notion of the state as a distinct regional entity, affording it membership within the international order. Any dismantling of state sovereignty under the traditional concept would lead to the disintegration of the international community itself, weakening its functionality [3].

1.1. Methodology Plan

Objective. Clearly state the purpose of the article, which is to explore the legal challenges associated with cyber sovereignty.

Research Questions. Pose the central questions the article aims to answer, such as: How does cyber sovereignty differ from traditional sovereignty? What are the unique legal challenges posed by cyber sovereignty?; and How can existing legal frameworks be adapted to address these challenges?

1.2. Literature Review

Traditional Sovereignty. Review key literature on traditional sovereignty, including its definition, scope, implementation, and legal frameworks (Renwick & Swinburn, 1992; Tsagourias, 2021).

Cyber Sovereignty. Summarize existing research on cyber sovereignty, highlighting how it is defined and implemented differently from traditional sovereignty (Bellanger, 2011; Laguerre, 2004).

Comparative Analysis. Compare and contrast the existing studies on traditional and cyber sovereignty to highlight the key differences and similarities.

1.3. Conceptual Framework

Defining Key Terms. Clearly define key terms such as «sovereignty», «cyber sovereignty», «traditional sovereignty» and «jurisdiction».

Framework Development. Develop a conceptual framework for understanding cyber sovereignty in the context of traditional sovereignty, emphasizing areas such as scope, implementation, control, and disputes.

1.4. Research Methodology

Approach: Adopt a qualitative research approach, using comparative legal analysis to examine the differences and similarities between traditional and cyber sovereignty.

Challenges and Disputes: Nature of Disputes: Identify and analyze the types of disputes states face in traditional sovereignty (regional conflicts, border security) versus cyber sovereignty (cybersecurity threats, internet governance conflicts); Role of Actors: Discuss the roles of various actors in traditional sovereignty (states, international institutions) versus cyber sovereignty (private sector entities, technology companies); Legal Challenges: Identify specific legal challenges in applying traditional sovereignty principles to cyberspace, such as jurisdictional issues, cross-border data flows, and enforcement difficulties.

1.5. Discussion

Interdependence: Discuss the interdependence between traditional and cyber sovereignty, emphasizing how principles of traditional sovereignty can inform the development of cyber sovereignty; Adaptation of Legal Frameworks: Propose ways to adapt existing legal frameworks to better address the unique challenges of cyber sovereignty, including potential new laws and international agreements; Future Directions: Suggest areas for future research and potential developments in international law to accommodate the evolving nature of cyber sovereignty.

2. Challenges Related to the Concept of Cyber Sovereignty

Legal concepts form the material structure of legal meaning, delineating its scope and functional context. The legal concept plays a crucial role in the application and enforcement of laws across various legal domains, as it serves as the foundation for interpreting, understanding, and implementing laws by legal practitioners, judges, and law enforcement authorities. Therefore, it is essential to address the conceptual challenges posed by cyberspace to the concept of sovereignty.

Defining what falls within the concept of sovereignty in international law can be a challenging task due to its dual nature. On one hand, sovereignty relates to the internal affairs of a state, defining the powers of public authority and its ability to regulate within state borders. On the other hand, it pertains to the external relations of the state, determining its relationships with other states in the international system.

Krasner (1999) provides a useful classification of sovereignty for our analysis. He identifies four ways to understand sovereignty: internal sovereignty, which refers to how public authority practices are organized and its ability to control within state borders; reciprocal sovereignty, which denotes the mutual compliance between the public authority of one state and that of another state to control the flow of people, materials, and ideas across borders; legal international sovereignty, which refers to the mutual recognition between states in the international system; and Westphalian sovereignty, meaning that each state has the right to determine its political life without external interference [4].

From our perspective, Krasner's classification deconstructs the concept of sovereignty into useful theoretical components. However, such deconstruction is not necessary for us when discussing the concept of cyber sovereignty. Therefore, for elucidating the meaning of cyber sovereignty, we will simplify the types of sovereignty to two: internal sovereignty, which refers to the relationship between the authority and its people, and international sovereignty, which refers to the relationship between the state and the international community.

The cyber environment influences internal sovereignty when the state loses the necessary control over the influx of external influences on societal harmony through the internet. International sovereignty of the state is affected when the flow of these external influences result from deliberate interference by one state in the affairs of another state.

Concept of cyber sovereignty directly poses two types of challenges to the stable concept of sovereignty in legal jurisprudence: the first challenge is distinguishing between the two concepts, which may appear similar but are distinct. Despite their points of convergence, they are not synonymous but rather one may subsume the other. The second challenge arises from the impact of cyberspace on defining sovereignty, as it alters the elements upon which the traditional concept of sovereignty relies. The latter focuses on power and its institutions, while cyber sovereignty necessitates the power of the people, as we will explain next.

2.1. Approaching Cyber Sovereignty in Comparison to Traditional Sovereignty

Is cyber sovereignty the same as traditional sovereignty? We need to answer this question before discussing the legal challenges of cyber sovereignty in international and national law, as the later discussion will rely on the elements and vocabulary of sovereignty in the traditional concept.

In approaching the concept of cyber sovereignty to traditional sovereignty, we conclude that they are not synonymous in meaning. Traditional sovereignty is broader and more comprehensive than cyber sovereignty in terms of scope and implementation. While traditional sovereignty refers to a state's supreme authority over its territory, people, and government, and its ability to enact and enforce laws within its borders [8], cyber sovereignty refers to a state's authority and control over activities occurring within its cyber space, including cyber networks and the flow of data and content over the internet. It is confined to the virtual world.

On the other hand, a state's general sovereignty is confined by geographical boundaries and territorial jurisdiction, where the state exercises control over what happens within its borders. However, the link between the concept of borders and cyber sovereignty working in a borderless environment renders traditional borders less significant.

In terms of the scope of authority, traditional sovereignty relates to a state's authority over its physical territory, encompassing aspects such as governance, law enforcement, defense, and international relations [5], while cyber sovereignty's meaning is limited to a state's authority over its cyber world within its borders. It is noted that borders remain relevant in cyber sovereignty, as the state's legitimate authority over its cyber space is limited to controlling this space within its borders. However, regulating these borders is only partially and technically feasible, necessitating urgent international cooperation among states in this regard.

In matters of control and regulation, traditional sovereignty includes governing physical territories through established legal and political institutions, involving tangible control over actual territories, borders, and populations, relying on a reliable legal framework and physical infrastructure for governance. Cyber sovereignty, on the other hand, includes control over its cyber space through regulatory frameworks, laws, and technical measures to control activities over the internet and data flows within the state's jurisdiction, such as cyber laws, regulations, technical measures, and cooperation with internet service providers and technology companies [11].

They also differ in disputes that states face in exercising their sovereignty. In traditional sovereignty, states face issues of regional conflicts, border security, and external threats to national sovereignty, while in cyber sovereignty, states face different issues related to the nature of the virtual world, such as cyber security threats and conflicts over internet governance.

In terms of relationship, parties in traditional sovereignty are other states and international institutions, while parties in cyber sovereignty are predominantly companies and entities in the private sector.

In terms of legal and political frameworks, traditional sovereignty is supported by reliable legal principles and international treaties regulating state behavior and relations, while cyber sovereignty still requires the development of new legal and political frameworks specifically designed for the cyber space, including data protection laws, international agreements on cyber standards, and cross-border cooperation.

The core argument of this text is that cyber sovereignty, while related to traditional sovereignty, is distinct and narrower in scope. To understand the legal challenges posed by cyber sovereignty, it is crucial to differentiate it from traditional sovereignty and analyze its unique characteristics and implications.

1. Definition and Scope: (a) Traditional Sovereignty: Refers to a state's supreme authority over its physical territory, people, and government, encompassing governance, law enforcement, defense, and international relations. It is defined by geographical boundaries and territorial jurisdiction; (b) Cyber Sovereignty: Involves a state's control over activities within its cyberspace, including data flow and internet content. It is confined to the virtual world and operates in a borderless environment, making traditional geographical boundaries less significant.

2. Implementation and Authority: (a) Traditional Sovereignty: Implemented through physical control over territories and populations, supported by legal and political institutions, and enforced via tangible means such as military and police; (b) Cyber Sovereignty: Exercised through regulatory frameworks, cyber laws, and technical measures within cyberspace. This includes cooperation with private sector entities like internet service providers and technology companies to regulate and control cyber activities.

3. Challenges and Disputes: (a) Traditional Sovereignty: States face regional conflicts, border security issues, and external threats. Sovereignty disputes often involve physical territory and populations; (b) Cyber Sovereignty: States encounter cyber security threats and conflicts over internet governance. Disputes are more about controlling cyber activities and ensuring data protection within a state's cyber jurisdiction.

4. Relationships and Actors: (a) Traditional Sovereignty: Interactions primarily involve other states and international institutions, governed by established international treaties and legal principles; (b) Cyber Sovereignty: Interactions predominantly involve private sector entities, such as tech companies and internet service providers, necessitating new legal and political frameworks tailored to the digital environment.

5. Legal and Political Frameworks: (a) Traditional Sovereignty: Supported by longstanding legal principles and international agreements that regulate state behavior and relations; (b) Cyber Sovereignty: Requires the development of new legal and political frameworks, including data protection laws, international cyber standards, and cross-border cooperation agreements.

6. Interdependence: (a) Traditional and Cyber Sovereignty: While cyber sovereignty is a subset of traditional sovereignty, addressing cyber sovereignty issues will rely on the principles and frameworks of traditional sovereignty. This includes regulating cyberspace, protecting national interests, and fostering international cooperation in cyberspace governance and law enforcement.

The analysis reveals that while cyber sovereignty shares foundational principles with traditional sovereignty, it presents unique challenges and requires specific legal and regulatory frameworks. Traditional sovereignty provides a basis, but the distinct nature of cyberspace necessitates tailored approaches to governance, security, and international cooperation. Understanding these differences is essential for addressing the legal challenges of cyber sovereignty in both national and international contexts.

In summary, while traditional sovereignty concerns a state's authority over its territory, people, and government, cyber sovereignty pertains to one aspect of a state's exercise of its authority over its territory, people, and government. When we later discuss the concept, scope, and implementation of cyber sovereignty in international and national law, we will undoubtedly do so within the frameworks provided by traditional sovereignty, as recognized by international agreements and national laws when extending the concept of sovereignty to application in cyberspace, in areas of regulation,

control, protecting national interests, and addressing specific challenges such as internet governance, law enforcement, and international cooperation.

2.2. Partial Displacement in Dynamics of Sovereignty from the Power of Authority to the Power of the People

There is necessity of sovereignty for state formation and combination of the elements of land and people. There is also necessity for peoples to use it as a wall protecting their independence and identity towards other countries [7]. Despite of that, the matter is not without complexity in the relationship between the people as a source of authority and the state institutions that represent them and exercise these authorities. People precede the state and are the end goal, while the state is the means. People see themselves in a superior position because sovereignty is at their service, while the state sees itself in a superior position because it realizes the people's need for it. This makes the relationship between the people and sovereignty a state of tension and attraction, only resolved by the law agreed upon by society through proper legislative mechanisms satisfactory to the people.

Stable legal mechanisms give legitimacy to state institutions to exercise sovereignty over the people, represent them to other countries, and protect their interests. However, legal mechanisms are influenced over time by power dynamics and control, which are essential to the concept of sovereignty [6]. One of the latest dynamics is the emergence of cyberspace and its ability to connect and influence people without passing through the gates of power and control.

Foucault (1980) believes that the control of power over its internal conditions and the realization of sovereignty does not stop at possessing legitimacy of restriction and accountability but is essentially achieved through the management of knowledge and information. This is precisely what makes cyberspace potentially contradictory to the concept of sovereignty even before it poses a challenge to it in its implementation [9].

Achieving sovereignty requires the state to be ahead of the people in managing knowledge and information to perform its function, while cyberspace injects information in a way that puts individuals on a parallel interaction level with the state's interaction. It goes further by influencing individuals' motives to act and take positions. The key here is the antagonistic relationship between information and control: those who monopolize their information exert more control, while those whose information spreads have less control [15].

What is said about information can be applied to knowledge, with the difference being that information has a momentary impact in the short term, whereas knowledge affects societies in the long term and to a deeper extent than information.

In the context of cyber sovereignty, questions arise about individuals' consent to state intervention in their online activities, the boundaries of state authority in regulating cyberspace, and the rights and responsibilities of individuals in the digital age. Foucault's insights into knowledge and sovereignty revolve around his analysis of disciplinary mechanisms and systems of power. He emphasizes that power operates not only through coercion and repression but also through knowledge and discourse.

Regarding sovereignty, intellectuals offer a critical perspective challenging traditional concepts of state power. They question the idea of the existence of a centralized sovereign power and instead explores how power operates in dispersed and varied ways through networks of knowledge and practices. For example, Foucault's concept

of governmentality refers to the techniques and strategies used by institutions and authorities to govern populations [9].

Power is a tool for exercising sovereignty. Although the contradiction between knowledge and power takes time to manifest its impact, its solid influence makes it difficult for power to change its direction. It can be said that the flow of information from cyberspace disrupts the work of power, while the evolution of knowledge threatens the existence of power itself if it does not adapt with new knowledge. It is in the interest of power to move in the same direction as the people (democracy) rather than trying to prevent them from evolving due to interaction with knowledge coming from cyberspace (dictatorship).

States acknowledge this reality; hence they take precautions in dealing with the information and knowledge dictated by cyberspace, attempting to prevent, manipulate, or respond to it. They do this because of their continuous sense that cyberspace poses a constant threat to their sovereignty. Thus, the new concept of «cyber sovereignty» emerged as an attempt to address this threat. Some countries, like China, have taken it further by isolating their people from the global cyberspace and confining them to a cyberspace exclusive to Chinese territories, delaying or avoiding the challenge of information flow and the development of knowledge among the people outside the gates of power.

This challenge to power is a challenge to the law because it makes the power of the people a counterforce to the power of the ruling authority. It may constitute an opposing force that changes either the power itself or the laws through which power operates. The change could be abrupt, replacing or delegitimizing power, or it could be slow and indirect, focusing on developing national laws on which power relies. This is because there are hidden yet close links between the state of information and knowledge provided by cyberspace and the law and the public order. Despite their global dimension, morals and values, as well as their acknowledgment, scope, and practice, differ from one society to another. Even virtues have a different perspective from one society to another. These differences, influenced by cyberspace, challenge national laws that protect values, rights, and freedoms in issues such as privacy, freedom of expression, and personal liberty.

Returning to the concept of sovereignty, we conclude that it is not just political control exercised by the state, but a complex process intertwined with systems of knowledge, discourse, and social values that constantly seek to regulate individual behavior. In general, Michel Foucault's analyses of knowledge and sovereignty offer valuable insights into the complex relationship between power and knowledge production in modern societies.

In this sense, the widespread participation in information and knowledge due to cyberspace, and its impact on the relationship between the people and the authorities, partially takes some tools of the state in exercising its sovereignty and puts them in the hands of individuals. It diminishes the gap in knowledge between the people and the sovereign state institutions regarding the management of their affairs and levels of representation. In this sense, people's sovereignty, which was once legitimatized and only achieved through the state, becomes a reality that allows individuals to intervene in the tools of these institutions' work and affects their ability to control. This not only changes the exercise of sovereignty but also partially changes the concept of sovereignty itself because the role of the people in the traditional concept of sovereignty is

only realized through state institutions [10]. In cyber sovereignty, the people indirectly become partners intervening in the management of knowledge and information, making it a guiding material for societal and political positions without passing through the gates of power.

States are rigid entities, and societies are interactive entities. States work to regulate the general rhythm, while societies escape from it, although they recognize their need for it. This is because states are driven by the motives of control, sovereignty, and societies are driven by the motives of cultural freedom.

3. Challenges Related to the Application of Cyber Sovereignty

When we apply the concept of cyber sovereignty discussed here to real-world applications, we find clear parallels with traditional sovereignty, where states have exclusive authority and control over their physical territories, including land, air, and territorial waters. International law recognizes the principle of territorial sovereignty, granting states the right to exercise jurisdiction and governance within their borders without external interference. Traditional sovereignty governs legal principles established in international law, including the United Nations Charter, customary international law, and treaties such as the Vienna Convention on Diplomatic Relations and the Montevideo Convention on the Rights and Duties of States.

However, when attempting to apply cyber sovereignty to include a state's authority in cyberspace, we find ourselves in a borderless realm where cyber activities often transcend traditional national boundaries. How then do we apply sovereignty in cyberspace? International law regarding cyber sovereignty is still evolving and lacks clear consensus, but states seek to apply the principles of traditional sovereignty in cyberspace despite ongoing debates about states' ability to control the global internet and effectively address cross-border cyber issues.

We will first present cyber sovereignty in the international system, then return to cyber sovereignty in the national system. This is because we believe that the concept of sovereignty first emerged within the framework of the international system before extending to the national system, which was previously satisfied with the concept of authority. However, before proceeding, we need to answer an introductory question: Does cyber sovereignty fall within the traditional concept of sovereignty? This is our initial challenge.

3.1. Cyber Sovereignty in International Law

Sovereignty is a fundamental concept in the current international system, representing authority within a distinct territorial entity and affirming a state's membership in the international system. Steven Krasner classifies sovereignty into four types: domestic sovereignty, interdependence sovereignty, international legal sovereignty, and Westphalian sovereignty.

Cyber sovereignty in the international system refers to a state's complete control over its cyber domain, including the internet, information, data, and other systems. In this context, cyber sovereignty is part of a state's traditional national sovereignty, reflecting its ability to maintain independence, control over electronic systems, and protection of national interests in cyberspace.

Concepts of cyber sovereignty include a state's right to determine internet policies and regulations, safeguard national cyber networks' security and safety, enforce laws and regulations related to cybercrimes, protect citizens' and businesses' sensitive data, and cooperate with international entities to combat cross-border cyber threats.

This reflects sovereignty's concept over national borders, where states have exclusive control over their territories and citizens, including legal, political, economic, and military authority, a fundamental rule of the current international system where each state has an absolute right to determine its destiny and implement its policies within its national borders without undue external interference.

No state has formally acknowledged the independence of cyberspace [12]. Although, the absence of territorial boundaries in cyberspace enables states to impose a degree of territoriality by implementing control mechanisms to safeguard information flows across their borders. We can provide the illustrative case of Yahoo!'s refusal to comply with France's request to cease auctioning items associated with Nazism, citing the internet's self-regulating nature. Subsequently, a French court demonstrated that the American company was not operating in a legal vacuum but was conducting business in France, where promoting Nazism is prohibited under criminal law.

However, international sovereignty must have its limits and constraints, as states must adhere to principles of international human rights and laws and refrain from using their sovereignty in ways that contradict the interests of other states or international peace and security.

Cyber sovereignty remains a contentious issue in the international system, particularly with the rise of government and non-governmental cyberattacks and new technological challenges facing states.

According to the United Nations expert report (GGE Report 2013, UN Doc A/68/98; GGE Report, A/70/174), states acknowledge that international law, including the principle of sovereignty, applies to cyberspace, considering that «the international standards and principles stemming from state sovereignty apply to the use of information and communications technology by states and to their respective judicial authorities in the information and communications technology infrastructure.

However, this is not enough to recognize cyber sovereignty in international law for the first issue, namely «sovereignty as a rule-based system». The controversial point is whether sovereignty should only be considered as a principle from which legal rules are derived, or as a separate binding rule in international law.

The United Kingdom supported the first approach. Specifically, during his speech «The Internet and International Law in the Twenty-First Century». Attorney General Jeremy Wright claimed that although sovereignty is fundamental in the rule-based international system, it is not possible to «derive a specific rule or additional prohibition on electronic activity from this general principle of non-intervention. Therefore, the position of the United Kingdom government is that there is no such rule under current international law». Following this logic, electronic infiltration without crossing the threshold of the non-intervention principle can only be considered unfriendly, but it will not constitute a violation of international law. Accordingly, in the context of the internet, sovereignty cannot be considered a fundamental independent rule, but rather a fundamental principle of international law that guides relations between states.

Most states have expressed conflicting positions. Among them, the Netherlands considers that «respect for the sovereignty of other states is an obligation, and its violation may constitute an international wrongful act» (National Position of the Netherlands, p. 2). Finland also notes that «by agreeing that hostile electronic operations without crossing the prohibited intervention boundaries cannot constitute an international wrongful act, especially as such operations are not regulated, and the targeted state is

deprived of a significant opportunity to claim its rights». Therefore, a breach of sovereignty, considered as a fundamental rule in international law, «constitutes an international wrongful act and leads to state responsibility» (National Position of Finland, p. 3).

Regarding the Principle of territoriality, In general, national borders are an essential element in embodying the concept of sovereignty, as they determine the territory over which the state exercises its powers, protects its interests, and maintains its independence in crucial areas such as legal jurisdiction; protection of political, economic, and security national interests; control over natural, economic, and cultural resources, including their use and wealth distribution among citizens; regulation of immigration and passage for the movement of people and goods; and enforcement of laws related to immigration and customs; and national identity and belonging, as they contribute to building cultural, social, and political links between citizens [14].

Therefore, borders represent two things: they are a component of sovereignty as a concept and are defined for the territorial jurisdiction of states' sovereignty, and without them, the concept of sovereignty disintegrates, and its scope disappears. Therefore, it is not surprising that we attempt to subject the open cyberspace to the concept of closed national borders, necessitating the definition of cyber sovereignty, and addressing the challenges facing sovereignty as a concept and its application in the cyber environment.

3.2. Cyber Sovereignty in National Law

Implementation of Sovereignty in national law refers to the concept that emphasizes the right of states to govern and control the cyberspace within their borders, including regulating the flow of information, enforcing laws, ensuring cyber security, and protecting national interests in that space. It underscores the authority of the state in establishing and implementing its own rules and regulations related to internet activities and user behavior online within its legal jurisdiction. Cyber sovereignty emphasizes the importance of national control and independence in managing cyber affairs, while also recognizing the interconnected and global nature of the internet.

The concept of cyber sovereignty raises numerous legal issues within the scope of national law, including the applicable law in disputes between individuals, the jurisdiction competent to hear these disputes and its scope, as well as challenges that cast shadows on freedoms and human rights.

Legal and Jurisdictional Authority: The borderless nature of the internet poses challenges regarding judicial jurisdiction, determining which laws apply to online activities that may span multiple jurisdictions can be complex, leading to conflicts between different legal systems and uncertainty about which country has the authority to regulate certain online activities.

Data Protection and Privacy: With the continuous increase in the amount of personal data transmitted and stored online, issues related to data protection and privacy become crucial. Countries differ in the laws and regulations governing data protection and privacy, leading to challenges in ensuring consistent protection of individuals' data across borders.

Freedom of Expression: Striking a balance between the right to freedom of expression and the need to regulate harmful content online poses a legal challenge. Some governments may use the concept of cyber sovereignty to justify censorship and re-

strictions on online content, raising concerns about violations of the right to freedom of expression and access to information.

Cybersecurity: Ensuring cybersecurity within national borders, in addition to international cooperation to address cyber threats, is a complex legal issue. Cyberattacks can originate from anywhere in the world, making it difficult to determine responsibility and enforce legal measures against perpetrators.

Cross-Border Data Flow: Many companies and services rely on cross-border data flow to operate efficiently. Legal issues related to data localization requirements, restrictions on cross-border data transfers, and ensuring the free flow of data while protecting data privacy and security are raised.

Dealing with these legal issues requires international cooperation, dialogue with relevant stakeholders, and the development of frameworks [13].

4. Navigating the Legal Landscape: Analyzing the Key Challenges to Cyber Sovereignty

Since the Treaty of Westphalia in 1648, the model of the modern nation-state has become clear, and the concept of national sovereignty has been legally established and upheld by nations, as affirmed by the United Nations Charter, while considering the measures of Chapter VII. However, cyberspace has emerged as a real challenge to this concept of sovereignty. The historical foundation laid by the Treaty of Westphalia underscores the traditional concept of state sovereignty, where nations have supreme authority within their territorial borders, a principle enshrined in the UN Charter. This well-established framework, however, is significantly disrupted by the advent of cyberspace, which inherently lacks geographical boundaries and thus challenges the conventional notions of jurisdiction and state control.

It may seem that the threat to sovereignty arises from interaction between states, but the reality is that the challenge posed by cyberspace to state sovereignty comes from within the states themselves. Cyberspace affects states before it affects their societies, as data and information flow into them in the form of news, goods, services, values, and cultures. Unlike traditional sovereignty threats, which typically involve external actors, the threats from cyberspace originate internally, as the digital domain permeates the social fabric of nations, altering how information, culture, and values circulate within society. This internal disruption can lead to shifts in public opinion and societal norms, which may clash with state institutions and policies, thereby weakening the internal cohesion that underpins state sovereignty.

The impact of cyberspace contents on societies may change collective public opinion and incite and direct masses at a historical moment, where the views of state institutions clash with a portion of their society, creating a conflict between them. This conflict weakens the concept of sovereignty from within, not to mention the problem and scope of applying national law to the national public order, understanding the laws that must be applied, recognizing judicial jurisdiction, and preserving security, privacy, and human rights. The capacity of cyberspace to rapidly influence public opinion poses a significant threat to state authority, as digital platforms can mobilize dissent and challenge governmental policies, leading to internal conflicts. These conflicts highlight the difficulty states face in applying national laws to regulate online activities, maintaining public order, and safeguarding rights in a digital context where traditional legal frameworks may be inadequate.

States still cling to the concept of sovereignty and refuse to weaken it due to the cyberspace reality that threatens the concept of national borders. These borders seem easily crossed in cyberspace, opening wide interaction between societies in an unguided context. Then comes the fact of manipulating individuals' choices through indirect guidance through media and influencing public opinion and inciting crowds by stirring their own motivations in each society, and the individual tendency to escape from the exercise of the state's sovereign role in law enforcement. Despite the erosion of physical borders in cyberspace, states remain steadfast in their commitment to preserving sovereignty. This persistence is challenged by the ease with which information and influences traverse digital boundaries, often leading to manipulation of public sentiment and behaviors without state mediation. The ability of digital media to guide and incite public opinion further complicates state efforts to exercise control and enforce laws, as individuals increasingly resist traditional forms of state authority in favor of the freedoms offered by cyberspace.

The legal challenges to cyber sovereignty affect the economic, social, political, and security revenues of any state, and they are dealt with political and security tools more than they are confronted with legal tools. International law still lacks effective regulatory frameworks in this regard. The multifaceted impact of cyber sovereignty on various state functions — economic stability, social cohesion, political integrity, and national security — demands robust responses. However, states often resort to political and security measures, such as surveillance and censorship, rather than developing comprehensive legal solutions. The inadequacy of international legal frameworks to effectively regulate cyberspace exacerbates these challenges, underscoring the need for innovative legal and cooperative international approaches.

In the quest for legal solutions to these challenges, we must return to the deep concept of state sovereignty, where sovereignty originates from the community, not the state, and the purpose of granting it to the state is for it to represent the community and reflect its will in line with human values and the society's culture, beliefs, and choices. The state's duty is to adhere to sovereignty to fulfill its functional role as a representative and protector of society. Revisiting the fundamental principle that sovereignty is derived from the people and conferred upon the state to act as their representative highlights the importance of aligning state actions with the will and values of its citizens. This perspective implies that addressing cyber sovereignty challenges requires states to enhance their engagement with communities, ensuring that digital governance reflects collective societal interests and protects individual rights.

In this context, between the concepts of society, state, and cyber sovereignty, lie two authentic concepts, namely freedom and culture. Freedom is the highest and most attractive value in cyberspace interactions, yet it is also the biggest challenge as it defies societal restrictions on individuals through sovereignty. As for culture, it defines the form and direction of collective movement in societies and determines their possibilities and scenarios. It will also determine the internal interaction of society with sovereign national institutions. Freedom and culture are integral to the discourse on cyber sovereignty. Cyberspace amplifies individual freedoms, often challenging societal restrictions imposed through state sovereignty. Balancing these freedoms with the need for societal order is a key challenge. Culture shapes how societies engage with cyberspace and influences their responses to state regulation, affecting the efficacy of sovereign control and legal frameworks.

States will always attempt to control the flow of information. Electronic packets cannot escape this practice (Deibert & Dombroski, 2011). Recent developments show that states are trying to overcome the contradiction of borders and define boundaries by asserting sovereignty over cyberspace [14]. Despite the borderless nature of cyberspace, states persist in their efforts to control information flows. These efforts are evident in various measures, such as internet censorship and digital surveillance, aimed at defining digital boundaries and asserting sovereignty. The ongoing struggle to reconcile the traditional concept of borders with the realities of cyberspace reflects the dynamic and evolving nature of cyber sovereignty, necessitating continual adaptation and innovation in legal and regulatory approaches.

5. Conclusion

In conclusion, we can infer that the concept of cyber sovereignty is not synonymous with traditional sovereignty but rather represents an evolution in the concept of sovereignty arising from technological advancements and current circumstances. While traditional sovereignty focuses on authority and actual control within geographic borders, cyber sovereignty emphasizes authority and control in cyberspace and the flow of data over the internet.

The application of the concept of cyber sovereignty in international and national law holds significant importance in dealing with the new challenges posed by modern technology and the internet. This concept is an integral part of national sovereignty, affirming the right of states to control and regulate their own cyberspace through the organization and enforcement of laws and regulations pertaining to the internet and data. States can thus maintain their cyber security and protect their national interests in this space. However, this also requires international cooperation and the development of an appropriate international legal framework to address common challenges and ensure stability and security in the interconnected and global cyberspace.

History tells us that castle walls once protected cities and civilizations by force from hostile incursions and movements of chaos. Then national borders did so through law, until the open cyberspace demolished the walls and always opened the borders to the flow of everything. Thus, states wishing to protect their sovereignty have no choice but to rely on the culture and awareness of their peoples. The cultures of nations have become walls and national borders, protecting their sovereignty based on human values, freedom, and law. We call on communities to build their sovereignty through a culture of respect for the law that represents them, and we call on states to work towards establishing effective international regulatory frameworks to ensure the free operation of cyberspace while respecting sovereignty.

The legal challenges of cyber sovereignty entail precise understanding of the dynamic interactions in cyberspace and the development of a suitable legal and legislative framework to achieve a balance between national control and international cooperation in this field.

In summary, the legal challenges of cyber sovereignty require a comprehensive understanding of the dynamic interactions in cyberspace and the development of an appropriate legal and legislative framework to achieve a balance between national control and international cooperation in this field.

References

1. Adams J. & Albakajai M. (2016) Cyberspace: A New Threat to the Sovereignty of the State. University of Essex Research Repository. Management Studies. Nov.-Dec. Vol. 4. No. 6.
2. Schneider G. (2013) E-Business, 10th ed. London: Course Technology, Cengage Learning.
3. Kuehl D. T. (2009) From Cyberspace to Cyberpower: Defining the Problem. Cyberpower and national security, 30.
4. Krasner S. D. (1999) Sovereignty: Organized Hypocrisy, Princeton: Princeton University Press.
5. Tsagouria N. (2021) Chapter 1: The legal status of cyberspace: sovereignty redux? Elgar online, 12.
6. Hinsley F. H. (1967) The Concept of Sovereignty and the Relations Between States. Journal of International Affairs. Vol. 21. No. 2.
7. Ong. (2012) Powers of sovereignty: State, people, wealth, life, Focaal, November.
8. Renwick & I. Swinburn. (1992) Upper Secondary School Valletta. Upper Secondary School Valletta. Hyphen. 7(2).
9. Michel Foucault. (1980) Power / Knowledge, ed. by C. Gordon. Pantheon Books. New York.
10. Mirza M., Ali L., Qaisrani I. (2021) Muhammad Nadeem Mirza1, Lubna Abid Ali2, Irfan Hasnain Qaisrani. Webology. Vol. 18, No. 5.
11. Bellanger P. (2011) From sovereignty in general to digital sovereignty in particular. In Les Echos.fr, 54, 30.
12. K. Ivanova, M. Myltykbaev, D. Shtodina. (2022) The Concept of Cyberspace in International Law // Law Enforcement Review. Dec. 2022.
13. Wu T. S. Cyberspace Sovereignty? The Internet and the International System. Harvard Journal of Law & Technology. 1997. Vol. 10. No. 3.
14. Heinegg von W. H. (2012) Legal Implications of Territorial Sovereignty in Cyberspace // 4th International Conference on Cyber Conflict. NATO CCD COE Publications. Tallinn.
15. Laguerre, M. (2004) Virtual time, in information. Communication & Society. 7(2).